Daily Security Maintenance Audit Checklist	Task	Responsible
Security Systems (IDS, Firewalls, VPN, Badging Systems, Security Cameras, Physical controls (locks), AntiMalware Systems, Email Security)		
	Capacity check	CISO/CSO, SecAnalyst
	Threat Feed check	CISO/CSO, SecAnalyst
	System log review	CISO/CSO, SecAnalyst
	Add/Moves/Changes that need to be reflected in docs.	CISO/CSO, SecAnalyst
Log Management		
SIEM		
	Traffic patterns & Activity overnight	CISO/CSO, SecAnalyst
	Foreign Country Activity	CISO/CSO, SecAnalyst
	Port Scans	CISO/CSO, SecAnalyst
Windows Server Event logs		
Check replication		NOC, SecAnalyst
Logon/Logoff	Review events	NOC, SecAnalyst
Network Infrastrucuture Syslogs		CISO/CSO, SecAnalyst
Operational logs		CISO/CSO, SecAnalyst
Sandboxing		
	Cyphort	CISO/CSO, SecAnalyst
	Fireeye	CISO/CSO, SecAnalyst
Web Security		
	Cisco WSA	CISO/CSO, SecAnalyst
	Cyphort	CISO/CSO, SecAnalyst
UBA (User Behavior) - Preempt		
Account Lockout	Triage previous nightly events	CISO/CSO, SecAnalyst
Priv Account Activity	Triage previous nightly events	CISO/CSO, SecAnalyst
Vulnerability Scans		
Nessus nightly scans	Review scan results	CISO/CSO, SecAnalyst
	Plan any remediation	CISO/CSO, SecAnalyst
Mobile Device Management		
Airwatch	Review activity logs	CISO/CSO, SecAnalyst
	New self enrollments	CISO/CSO, SecAnalyst
Monitoring Systems (non-SEIM)		
Solarwinds, WhatsupGold, …	Review logs	NOC, SecAnalyst
	Review fileshare permissions	NOC, SecAnalyst
	Review device uptime levels	NOC, SecAnalyst

Backup & Recovery

Server Backups	Review logs for falures	NOC Sys Engineer
Virtual Snapshots	Review for exisiting snapshots	NOC Sys Engineer
Routers/Switches	Review config failures	NOC Sys Engineer
Review backup		

Monthly Security Maintenance Audit Checklist	Task	Responsible
Server Hardware Health	Firmware checks	NOC - Sys Eng
	Driver checks	NOC - Sys Eng
	Hardware checks	NOC - Backup Eng
	Disk Space checks	NOC - Storage Admin
	Add/Moves/Changes that need to be reflected in docs.	NOC
	DNS Name	NOC - Sys Eng
Storage Networks		
	Firmware checks	NOC - Storage Admin
	Hardware checks	NOC - Storage Admin
	Disk Utilization Report\Capacity check	NOC - Storage Admin
	SAN HQ Report	NOC - Storage Admin
	Add/Moves/Changes that need to be reflected in docs.	NOC - Storage Admin
Virtual Infrastructure		
	Host Inventory	NOC - Sr. Sys Eng
	Guest Inventory	NOC - Sr. Sys Eng
	Application version checks	NOC - Sys Eng's
Core Network Devices (Switches/Routers/KVM)		
	Firmware checks	NOC- Network Architect
	Hardware checks	NOC- Network Architect
Security Systems (IDS, Firewalls, VPN, Badging Systems, Security Cameras, Physical controls (locks), AntiMalware Systems, Email Security)		
	Firmware checks	Security Analyst(s)
	Hardware checks	Security Analyst(s)
	Capacity check	Security Analyst(s)
	Threat Feed check	Security Analyst(s)
	System log review	Security Analyst(s)
	Add/Moves/Changes that need to be reflected in docs.	Security Analyst(s)
VOIP Systems		
	HQ Server check	NOC - Messaging Architect
	DVS check	NOC - Messaging Architect
	Phone check	NOC - Messaging Architect
	Inventory check	NOC - Messaging Architect
	SIPerator check	NOC - Messaging Architect
	QuickLook report	NOC - Messaging Architect
	Performance check	NOC - Messaging Architect
Wireless Networks		
	Inventory (Make, Model, Serial #, Service Tag, Location, Idiot lights)	NOC - Network Architect

	Warranty\Service Agreement check (Covered? Which contract?)	NOC - Network Architect
	Firmware checks	NOC - Network Architect
	Hardware checks	NOC - Network Architect
	Capacity check	NOC - Network Architect
	System log review	Security Analyst(s)
	Add/Moves/Changes that need to be reflected in docs.	NOC - Network Architect
	Performance check	NOC - Network Architect
Log Management		
SIEM		
	Event logs	Security Analyst(s)
	Syslogs	Security Analyst(s)
	Universal forwarder check	Security Analyst(s)
	Operational logs	Security Analyst(s)
UBA (User Behavior)		
	Application updates	Security Analyst(s)
	Review anomalous behavior	Security Analyst(s)
	Create updated reports based on above	Security Analyst(s)
Asset Management		
SCCM Inventory		
	Servers	Desktop Engineer
	Desktops	Desktop Engineer
	Laptops	Desktop Engineer
	Inbound inventory controls (aka stuff we need to replenish)	Desktop Engineer
Patch Management		
SCCM WSUS/3rd Party Solution	Server software upgrades	Desktop Engineer
	Review Inventory	Desktop Engineer
Backup & Recovery		
	Application & Agent Updates	NOC - Sys Engineer
	Review logs for failures	NOC - Sys Engineer
	Plan remediation for failures	NOC - Sys Engineer
Environmental Controls		
	HVAC Systems	NOC
	Watchdog controls (MDF/IDF temperature/humidity reporting)	NOC
Monitoring Systems		
	Up/Down (What's Up Gold)	
	Trending (Cacti)	
	Alerting (PagerDuty)	
	Review fileshare permissions	
	Review device uptime levels	

Database Systems		
	Database Inventory	NOC
	Database growth\capacity	NOC
	Database issue review	NOC
	Database security review	NOC
	Error log review	NOC
Change Management System		
	Review previous changes	CIO, CISO/CSO, Director
	Chart upcoming changs	CIO, CISO/CSO, Director
Password Management		
Thycotic		
Review autorolled passwords		
Data Loss Prevention		
	Review logs of activity	SecurityAnalysts
Vulnerability scans		
	Review reports and construct remediations	CISO/CSO, Security Analysts
Documentation		
	Review updates to documentation that need to be made	CIO, CISO.CSO, Directors, NOC
Mobile Device Management		
	Application & Agent updates	NOC, Security Analysts
	Review logs	NOC, Security Analysts
	Review release notes	NOC, Security Analysts
	Review usage/trends	NOC, Security Analysts
User Account Management		
	Review new accounts	NOC
	Review term'ed accounts	NOC
	Review AD admin accounts	Security Analysts
	Review AD accounts for non-employees	Security Analysts
	Review Service accounts	Security Analysts
	Looks at accounts across all systems (AD, Exchange, DMS, Voice Systems, VPN, Airwatch, Badging Systems, Cloud	Security Analysts, NOC
Documentation Management System		
	Review changes	NOC - Sys Eng
	Bulk imports/exports	NOC - Sys Eng
	Status checks	NOC - Sys Eng
	Document automation job review	NOC - Sys Eng
	Service trending	NOC - Sys Eng
	Capacity planning	NOC - Sys Eng
	Event logs	NOC - Sys Eng
Audio/Visual Systems		
	Inventory (Make, Model, Serial #, Service Tag, Location, Idiot lights)	Service Desk A/V Eng
	Warranty\Service Agreement check (Covered? Which contract?)	Service Desk A/V Eng

	Server Age check\Replacement Plan (When is expected retirement?)	Service Desk A/V Eng
	Projector bulb life check\replacement plan	Service Desk A/V Eng
	Firmware checks	Service Desk A/V Eng
	Hardware checks	Service Desk A/V Eng
	Review issues in the last month	
Messaging Platforms (Exchange, Mail Relay Services)		
	Review issues in the last month	NOC
	Review mail relay services report	NOC
Application Delivery MS SCCM		
	Deployments	Desktop Engineer
	Scripts	Desktop Engineer
	Audit PC list for boxes not getting updates	Desktop Engineer
	Audit PC's that aren't getting rebooted	Desktop Engineer
Faxing		
	Look at volumes	Service Desk
	Look for issues	Service Desk
	Track capacity	Service Desk
	Verify updates/release notes	Service Desk Manager
Critical Application Controls		
	Review performance of firm automation	NOC - Sys Engineer
	Review internal web sites	NOC - Sys Engineer
	Review IntApp jobs	NOC - Sys Engineer
	Review Finance System (Elite, Aderant, etc)	NOC - Sys Engineer
	Review DMS (iManage, OpenText, NetDocuments, etc)	NOC - Sys Engineer
**Include applications relevant to your firm*		
Training Systems		
	Updae all app's on Training machines	Desktop Engineer
	Verify no issues	Desktop Engineer
	Review new QRG's	Service Desk Manager
	Review new training videos	Training Manager
	Review LMS	Professional Development
Litigation Support		
	Review jobs this month	LitSupport Manager/Technicians
	Review iPro Systems for capacity	LitSupport Manager/Technicians
	Review licenses/use of software	LitSupport Manager/Technicians
	Review media tracking (Inbound Media log)	LitSupport Manager/Technicians
	Track open cases	LitSupport Manager/Technicians
AD Infrastructure		
	check replication	NOC, Security Analysts
	check dhcp	NOC, Security Analysts
	check dns	NOC, Security Analysts
	Review vcheck report	NOC, Security Analysts
	Review machine counts	NOC, Security Analysts

Linux Systems		
	Inventory (Make, Model, Serial #, Service Tag, Location, Idiot lights)	NOC, Security Analysts
	Warranty\Service Agreement check (Covered? Which contract?)	NOC, Security Analysts
	Server Age check\Replacement Plan (When is expected retirement?)	NOC, Security Analysts
	Firmware checks	NOC, Security Analysts
	Hardware checks	NOC, Security Analysts
	Capacity check	NOC, Security Analysts
	Threat Feed check	NOC, Security Analysts
	System log review	NOC, Security Analysts
	Add/Moves/Changes that need to be reflected in docs.	NOC, Security Analysts
	Performance check	NOC, Security Analysts
Endpoint Encryption		
	Review reports - look for any unencrypted systems	Desktop Engineer
	Review and document issues	Desktop Engineer, Security Analysts
Protected Power Systems		
	UPS - review reports	NOC - Network Architect
	PDU - verify connections\changes	NOC - Network Architect
MFD/Printer/Scanner/Copier		
	Inventory	Service Desk Manager
	Issue review	Service Desk Manager
Review conference Room technology		
	Review cables/technology in place	Service Desk A/V Eng
	Verify all systems are functioning (Crestron control panels, wireless keyboard, wireless	Service Desk A/V Eng